CASE STUDY

Cofense Case Study

Large U.S. Health Plan Administrator Conditions Employees to Protect Against Targeted Phishing Attacks

COFENSE

Cofense Case Study

COFENSE AND LARGE U.S. HEALTH PLAN ADMINISTRATOR

Background

The company is the largest third-party administrator of employee health plans and benefits in its four-state region. In business for more than 20 years, the company employs about 130 people and administers plans for nearly 75,000 members.

Executive Summary

Client: Large U.S. health plan administrator

Challenges: Too many users indiscriminately clicking links in suspicious emails, increasing the risk of a phishing attack.

Solutions: Cofense PhishMe SBE

Results: Susceptibility rates fell more than half, and IT no longer spends countless hours troubleshooting phishing-related issues.

Challenges

As an employee benefits administrator, the company handles its members' most sensitive data – personal health information (PHI) and employment benefits. Any phishing attack that compromises members' private data could seriously hurt the business. "In our world, phishing and educating our users about phishing is the No. 1 priority. That means we need to get people more involved and give them more tools to help them understand and recognize a phishing email," says the company's manager of IT and infrastructure.

> "In our world, phishing and educating our users about phishing is the #1 priority. That means we need to get people more involved and give them more tools to recognize a phishing attack."
>
> **— Manager of IT and Infrastructure, U.S.-based Health Plan Administrator**

While the company had averted attacks, the manager noticed some employees were clicking just about anything that crossed their inboxes. "They were clicking on emails they believed were genuine but that would wind up being phishing emails. Then it would take the IT department countless hours to rectify the problems," he recalls. Despite warning employees about phishing threats, "we weren't really seeing a change."

Recognizing the danger, he started looking for an anti-phishing solution that would prevent attacks while providing education about risks.

Solutions

Cofense PhishMe® SBE Implementation

In searching for an anti-phishing solution, he contacted the company's corporate parent for a recommendation. It turned out the larger organization was using Cofense PhishMe SBE and was very pleased with the results. "They were very happy to be a PhishMe client and told us we should give Cofense a call and try it out, so that's what we did."

Cofense PhishMe SBE is a cloud-based SaaS immersive learning platform that instructs users on the dangers of phishing through periodic simulations. Users who fail the test – by clicking on simulated phishing emails – receive instruction on how to identify, avoid, and report any threats they come across.

Before committing to Cofense PhishMe SBE, the company decided to do a trial run with two simulation scenarios. The change in susceptibility rates from the first to the second simulation was a "360-degree change," the IT and infrastructure manager says. "It was just amazing. After that trial, we knew we were sold. We went through the purchasing process, and we've been a Cofense client ever since."

Business Results

When the company ran its first simulation, more than one-third of its users failed the test, he recalls. Of 127 users tested, 46 clicked the simulated phish. "So, we knew we had a problem that needed to be addressed immediately."

The IT department followed up the simulation by disseminating instructional materials biweekly to users. "In the next six weeks, we went through the education process of shooting out education emails and having discussions internally with departments and departments heads," he says. When the second simulation was conducted, the number of users who clicked the simulated phish dropped to 21, less than half the original number.

Since then, the company has run simulations monthly, picking a different scenario each time. "With each scenario that we push out, we drop a couple more people off that list. However, I'm still seeing an issue with repeat offenders," he says. To address the issue, the IT department has been sending extra educational materials to the repeat offenders and then testing them with a rerun of the simulations they fail.

The process is working, he says. The overall number of users clicking simulated phishes is down to less than 10%, and he is working to shrink that to 1%. "We just continue to see the needle go the other direction, which is very good," he says. Another positive result, he says, is an increase in users notifying the IT department of phishing emails. "We are feeling more confident in our users as a line of defense for keeping our company secure and safe."

Real-world Scenarios

The company found that implementing Cofense PhishMe SBE was straightforward. The company had already loaded the solution for a trial, and the IT staff knew what to expect when it came time for the permanent installation. The biggest change was to organize the Cofense PhishMe SBE dashboard by department to help identify which groups of employees have the highest susceptibility rates and, as a result, require additional education.

To keep things fresh, and to reflect current real-world threats, Cofense frequently updates simulation scenarios. It's a useful practice, says the IT and infrastructure manager, who cited some recent HR-related phishing scenarios that were particularly helpful because they were similar to real phishes the company has seen. "The scenarios already built in are pretty amazing. They've hit basically everything that we as an IT department have seen come across in the past."

But even though the company's phishing susceptibility rates have dropped steadily, he says they ticked up with the most recent scenario. The simulation used a common phishing trick – a fake order confirmation for an online purchase. "Given that we are getting close to Christmas time and people are always ordering online, we wanted to see if people would click on this one. Of course our suspicions were confirmed, and we had a higher number of clicks compared to the prior simulation."

> "The scenario's already built in are pretty amazing. They've hit basically everything that we as an IT department have seen come across in the past."
>
> **— Manager of IT and Infrastructure, U.S.-based Health Plan Administrator**

Positive Reception

A technical support analyst with the company gives Cofense PhishMe SBE high marks for ease of use. After receiving a quick tutorial from the IT manager, the support analyst was ready to run the company's most recent simulation. "It was very easy for me to do," she says. As for user response, she says she's received nothing but positive responses.

The IT manager adds that some employees view it as a competition, while others clearly take pride in being able to identify simulated and real phishes. Increasingly, employees are getting better at notifying IT as soon as they see a suspicious email.

Conclusion

Company management has fully embraced the anti-phishing program. "The execs were on board from the beginning," he says. He keeps them up to date on simulation results, sharing with them monthly reports that break down susceptibility rates by group. "I sit down with the executives and walk through what trends we're starting to see, both negative and positive." Preparing the reports is easy, requiring only a few clicks to compile the necessary information and then formatting it as a PDF.

Based on his experience with Cofense PhishMe SBE thus far, the IT manager says he would gladly recommend it to peers. The educational and behavioral-conditioning components are especially valuable. "It's so user friendly and makes life easier. Having the education piece that Cofense provides is fantastic, and that would be my biggest talking point if I were recommending Cofense to another company."

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175